BRIEFING

EU Legislation in Progress

Updating the European digital identity framework

OVERVIEW

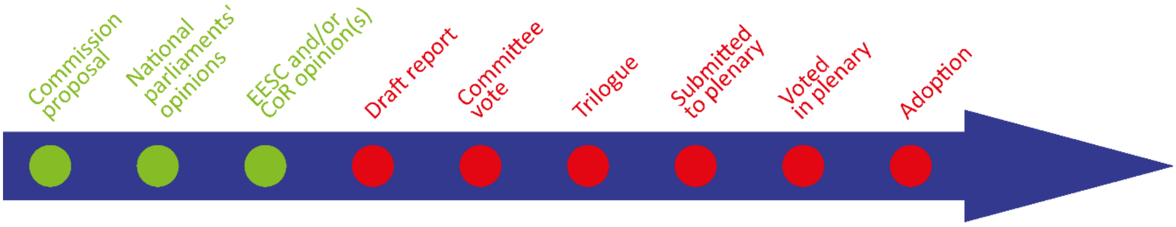
The 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation or eIDAS) was the first digital identity legislation to provide the basis for cross-border electronic identification, authentication and website certification throughout the EU. Application of eIDAS has been mixed. However, the pandemic increased the need for such solutions to be put in place to access public and private services.

On 3 June 2021, the Commission put forward a proposal building on the eIDAS framework, with the aim of giving at least 80 % of citizens the possibility to use a digital identity to access key public services by 2030 and to do so across EU borders. The updated European digital identity framework would also allow citizens to identify and authenticate themselves online without having to resort to commercial providers, a practice that raises trust, security and privacy concerns. In parallel, the Commission adopted a recommendation to design a toolbox supporting the framework so as to avoid fragmentation and barriers due to diverging standards.

Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE).

Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

Committee responsible:	Industry, Research and Energy (ITRE)	COM(2021)0281
Rapporteur:	Romana Jerković (S&D, Croatia)	3.6.2021
Shadow rapporteurs:	Riho Terras (EPP, Estonia) Mikuláš Peksa (Greens/EFA, Czechia) Dace Melbārde (ECR, Latvia) Elena Kountoura (The Left, Greece)	2021/0136(COD) Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Next steps expected:	Publication of draft report	



EPRS | European Parliamentary Research Service

Author: Mar Negreiro
Members' Research Service
PE 698.772 – October 2021

EN

Introduction

Since the pandemic began, the provision of public and private services has been becoming increasingly digital. Digitalisation can allow continued provision of what are often vital services (for example, in health care). The pandemic has greatly accelerated digitalisation, speeding it up globally by seven years, according to some analysts. This rapid digitalisation of services has inevitably increased demand for the digital provision of credentials, such as means for users to identify and authenticate themselves online. Governments and businesses alike need to adapt and serve customers and citizens digitally. However, access to public services and certain sectors (health, finance, etc.) requires identification or the exchange of attributes[1] with a high level of security and trustworthiness, including in terms of data protection. While secure identification systems are sometimes mandated by law, there is also increased demand for them, as most EU citizens would like access to a secure digital identity to use for online services. Moreover, according to Europol, the pandemic has significantly increased online identity fraud and other types of cybercrime.

Digital identity provision is undergoing fundamental changes. Entities such as banks, electronic communication service providers and utility companies, some of which are required by law to collect identity attributes, are leveraging their procedures to act as verified identity providers. There are many examples of European organisations using verified identities for their online services, many of which have been developed by banks, particularly in Scandinavian countries. Nevertheless, most are limited to national use and not available across the EU. Similarly, internet intermediaries, including major social media platforms and internet browser companies, also provide their users with digital identity services, mainly in the form of digital wallets.

With increased connectivity, mobile internet users also demand convenience and user-friendliness, including mobile-based digital identity solutions. In the EU, 86 % of the population are regular internet users, and about 74 % access the internet on the move from their mobile devices. Existing digital wallet solutions are typically linked to payment solutions (ApplePay, GooglePay, etc.), and allow users to store and link data in a single seamless environment on their mobile phones. However, some critics argue that this convenience comes at the cost of loss of control over personal data disclosed while these solutions are disconnected from a verified physical identity, which according to the Commission makes fraud and cybersecurity threats more difficult to mitigate.

Against this backdrop, the Commission put forward a proposal for a regulation on a framework for a European digital identity (EU eID).

Existing situation

For this initiative, the Commission has built on the existing Regulation on European electronic identification and trust services (eIDAS Regulation or eIDAS for short). Adopted in 2014, it provides the basis for cross-border electronic identification, authentication and website certification within the EU. Before the regulation entered into force, there was no comprehensive EU cross-border or cross-sector framework for secure, trustworthy and easy-to-use electronic transactions encompassing electronic identification (eID), authentication and trust services. However, the regulation is based on national eID systems that follow varying standards, and focuses on a relatively small segment of the electronic identification needs of citizens and businesses, namely secure cross-border access to public services. Moreover, there is currently no requirement for EU Member States to develop a national digital ID and to make it interoperable with those of other Member States, which leads to large discrepancies between countries. Today, 19 digital identification systems are used by 14 Member States. Furthermore, the regulation does not contain provisions on the use of such an identification for private services or mobile terminals, which leads to differences between countries.

At present, demand cannot be met by the eID means and trust services regulated by eIDAS, given its current limitations. Meanwhile, identification and authentication means developed by the private sector outside the eIDAS framework can only go so far in responding to the challenge. User-friendly third-party authentication services (for instance, using a Facebook or Google account to log in to different services) are common for accessing unregulated private online services that do not require a high level of security, but they cannot offer the same level of legal certainty, data protection and privacy, mainly because they are self-asserted and do not provide a link to trusted and secure government eIDs.

The report by the Commission's expert group on regulatory obstacles to financial innovation (ROFIEG) and the reports of the expert group on eID and know-your-customer (KYC) processes recognised that national regulatory bodies across the EU have different standards as regards the compliance of technical solutions for digital identity verification.

On 9 March 2021, the European Commission presented its vision for Europe's digital transformation by 2030. Its communication on the '2030 Digital Compass: the European way for the Digital Decade' announced an update of the Commission's overall digital strategy from February 2020 and of its gigabyte society targets, set in 2020 and 2016 respectively. The communication builds on the 2020 strategy on shaping Europe's digital future, which remains the overarching framework, while reconsidering the enormous changes brought about by the pandemic. It sets out a number of targets and milestones that the European digital identity will help achieve. For example, by 2030, all key public services should be available online, all citizens should have access to electronic medical records, and 80 % of citizens should use an eID system.

Parliament's starting position

In its October 2020 resolution on the digital services act and fundamental rights issues, Parliament highlighted that, while trusted electronic identification is elementary to ensure secure access to digital services and to carry out electronic transactions in a safer way, only about half of Member States have notified the Commission of their electronic identity scheme for cross-border recognition under the eIDAS Regulation. Parliament also stressed the unnecessary collection of personal data, such as mobile phone numbers, by online platforms at the point of registration for a service, often caused by the use of single sign-in possibilities. It underlined that the General Data Protection Regulation (GDPR) clearly describes the data minimisation principle,[2] and recommended that online platforms that support a single sign-in service with a dominant market share should be required to also support at least one open identity system based on a non-proprietary, decentralised and interoperable framework.

Council and European Council starting position

In its conclusions of 1-2 October 2020, the European Council asked the Commission to introduce an EU-wide digital ID system by 2021, to secure identification for the use of public and private online services. Similarly, reaching a general approach on the proposed regulation on a European digital identity is high on the agenda of the current Slovenian Presidency of the Council.

Preparation of the proposal

The initiative will build on the results of the ongoing review of the eIDAS Regulation, which is linked to the regulatory obligation for review included in Article 49 of the regulation. The Commission reviewed to what extent the eIDAS framework remains fit for purpose, delivering the intended outcomes, results and impact. It also considered whether it is appropriate to modify the scope of the regulation or its specific provisions, taking into account the experience gained in its application, and technological, market and legal developments. To that end, the Commission carried out an evaluation of the eIDAS framework, commissioned an external study, performed an impact assessment, and conducted an open public consultation, among other things. The results of these are described below.

Evaluation

The evaluation of the eIDAS framework revealed that the current regulation falls short of addressing new market demands. It builds on Member States' national electronic identity schemes notified under eIDAS. In the eIDAS Regulation, there was no requirement for Member States to develop a national digital ID or make it interoperable with those of other Member States, which led to large discrepancies between countries. Although the regulation has delivered on many of its goals and has become a fundamental element in facilitating the single market in a number of sectors (for financial services and enabling access and reuse of data in administrative procedures), it comes with a number of limitations. These include the lack of an obligation to notify national eID schemes, the limited attributes that can be reliably disclosed to third parties, the act's focus on the public sector, and the absence of clear incentives for private parties to use national eIDs. In addition, the evaluation found that the European electronic identity ecosystem is distributed across different national regulatory environments, levels of digital governance, cultures, and levels of trust in public institutions.

Impact assessment and study

On 30 July 2020, the Commission published an inception impact assessment with details of its plans to review the 2014 eIDAS Regulation from 2014. It concluded that the potential of electronic identification and authentication under eIDAS remains underexploited.

On 3 June 2021, the Commission published a study on the review of the eIDAS Regulation. This study supports the Commission's impact assessment (IA) in assessing the impact of different policy options to review the regulation, with the aim of establishing an updated legislative framework fit for purpose. The study took into consideration the input to the open public consultation conducted from 24 July to 2 October 2020 (see section below).

The study helps to define the problem, the policy options and the justification behind the need for EU legislative intervention in this field, and provides a comparative analysis of the costs and benefits expected for the stakeholders affected by the various policy options, namely: public authorities, online service providers, conformity assessment bodies, trust service providers, eID providers and wallet app providers.

The IA identifies three policy options. Under the baseline scenario (Option 0), the Commission would not propose any changes to the current legislation, and the eIDAS Regulation and its framework would therefore remain in force. To allow a consistent assessment and comparison of the options, the baseline also integrates the measures envisaged under secondary legislation that could be enforced without any changes to the regulation (e.g. non-adopted implementing acts) or positive spill-overs stemming from other pieces of legislation (such as the digital markets act).

Option 1 involved creating a European digital identity in the form of a strengthened legislative framework for national eIDs notified under eIDAS. It would require Member States to make eIDs available to all citizens and companies for cross-border use, and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. These measures would be taken without extending the scope of the eIDAS Regulation or affecting its underlying principles (i.e. they would be applicable to eID solutions notified by Member States, mutual recognition and technological neutrality).

Under Option 2, the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes across borders, such as proof of age (e.g. for accessing age restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences, medical test certificates, etc.

Option 3 would define a legal and technical framework for the deployment of the European digital identity as a user-controlled digital wallet app. The wallet app would empower users to securely share data related to their identity with public and private online service providers through their mobile devices, and allow them to control their own personal data. Further to legal requirements, common standards and/or technical references for the wallet app would be developed in close dialogue with Member States and private sector stakeholders.

The IA concluded that Option 3 stood out as the preferred one. According to the EPRS initial appraisal, the IA provides a good description of the main elements of the options.

The Regulatory Scrutiny Board (RSB) gave a positive opinion on a draft version of the IA report. However, the RSB considered that the IA did not provide a sufficiently clear explanation of the comparison between the policy options regarding their efficiency and effectiveness. Neither did the IA present the various views of the stakeholders sufficiently well.

Public consultation

As part of its review, the Commission also conducted an open public consultation from 24 July to 2 October 2020. The aim of the consultation was to gather feedback on drivers for and barriers to the development and uptake of trust services and eID in Europe. The consultation received responses from a total of 318 stakeholders. A large majority of respondents (60 %) said that they would gladly welcome the creation of a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities. For 57 % of respondents, the complexity of set-up and governance of a single and uniform European digital identity scheme was the main possible disadvantage. The overlap with existing solutions (49 % of respondents) and the lack of flexibility to adapt to technological developments and changing user needs (48 % of respondents) were also considered to be possible disadvantages.

The changes the proposal would bring

On 3 June 2021, the Commission published its proposal on a European digital identity framework based on the revision of the current one. With the proposal, the Commission hopes to meet the objectives of its digital compass, which stipulates that by 2030 all key public services are to be available online, all citizens are to have access to their digital medical records, and 80 % of citizens should be using a digital ID.

Furthermore, the Commission expects that the security and control offered by the updated European digital identity framework will offer everyone the means to control who has access to their digital ID and to which data exactly. This will also require a high level of security with respect to all aspects of digital identity provisioning, including the issuing of a European digital identity wallet, and the infrastructure for the collection, storage and disclosure of digital identity data. The proposal's specific objectives are to:

- provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand;
- ensure that public and private services can rely on trusted and secure digital identity solutions across borders;
- provide citizens full control of their personal data and assure their security when using digital identity solutions;
- ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.

The proposed framework for a European digital identity aims to achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid at European level. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules, and public administrations should be able to rely on electronic documents in a given format.

The proposal would address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use. It envisages a requirement for each Member State to issue a European digital identity wallet within 12 months after the regulation's entry into force. European digital identity wallets should be issued by a Member State, under a mandate from a Member State, or independently but recognised by a Member State. Thus, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (such as driving licence, diplomas or bank account). These wallets may be issued by public authorities or by private entities, provided these are recognised by a Member State.

The proposal does not impose any particular technology. The proposed European digital identity wallet would include the official identity data as issued by Member States and other identity attributes as electronic attestations of attributes. In its article 6a, the draft regulation requires Member States to follow compulsory compliance assessment and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act.

Also, the proposal lays down in article 6a(7) that the user should be in full control of the wallet, and establishes strict requirements for data protection and privacy for the issuer of the European digital identity wallet and for qualified providers of attestations of attributes, including compliance with GDPR requirements. Moreover, to ensure that users can identify who is behind a website, the proposal makes an amendment that would require providers of web browsers to facilitate the use of qualified certificates for website authentication. The conformity of European digital identity wallets with these requirements should be certified by accredited public or private sector bodies designated by Member States. By relying on a certification scheme based on the availability of standards commonly agreed among Member States, it should be possible to ensure a high level of trust and interoperability.

In parallel, the Commission adopted a recommendation so as to avoid fragmentation and barriers due to diverging standards. This recommendation will set out a process to support a common approach allowing Member States and other stakeholders from the public and private sectors, in close coordination with the Commission, to work towards the development of a toolbox. To meet the 12-month deadline for a European digital identity wallet to be issued in each Member State, this toolbox will accelerate the work by defining the technical architecture, common standards, and best practices and guidelines for the European digital identity framework.

Budget

The Commission will support the implementation of the European digital identity framework through the 'Digital Europe' programme, and many Member States have planned projects for the implementation of the e-government solutions, including the European digital identity, in their national plans under the Recovery and Resilience Facility. According to the Commission, the total financial resources necessary for the implementation of the proposal in the 2022-2027 period will amount to €30.8 million, including €8.8 million in administrative costs and up to €22 million in operational spending covered by the digital Europe programme. The financing will support costs linked to maintaining, developing, hosting, operating and supporting the eID and trust services' building blocks. It may also support grants for connecting services to the European digital identity wallet ecosystem, and the development of standards and technical specifications.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on the proposal, during its plenary session on 20-21 October 2021 (rapporteur: Tymoteusz Adam Zych, Diversity Europe – Group III/Poland). It highlights that the proposed digitalisation of services may result in the exclusion of parts of European society, in particular older people, those with low digital literacy and people with disabilities. It also notes that effective data protection needs to be considered in the context of the protection of fundamental rights, in particular the right to privacy and the right to the protection of personal data. The Committee agrees with the requirement that the European digital identity framework should give users the means to control who has access to their digital ID and what data can be accessed, while raising security concerns regarding the risks inherent in developing massive centralised systems that store and process sensitive data vulnerable to fraud and loss. The Committee therefore considers that users of European digital identity wallets should be guaranteed compensation for any undesirable situation relating to their data (e.g. data theft or disclosure).

The European Committee of the Regions (CoR) adopted an opinion on the proposal on 13 October 2021. Among other things the CoR calls for the wallet to be usable worldwide as a proof of EU identity, including features such as an official EU vaccination certificate or a digital deposit for visas. The CoR is however concerned about the security and technical risks posed by the centralised storage of identity data in a mostly mobile application. It therefore considers it important that the digital identity wallet be sufficiently reinforced against cyber-attacks. When it comes to the ID used for access by economic operators, the authorisation check should be designed with a secured certificate whose validity is of limited duration or cyclical. The Committee also asks for an extension of the implementation deadline for Member States from 12 to 24 months.

National parliaments

The proposal was open to review by the Member States' national parliaments. The deadline for the submission of reasoned opinions on grounds of subsidiarity was 4 October 2021. No reasoned opinions were submitted.

Stakeholder views[3]

Stakeholders' reactions have been divided on some issues. A selection of views expressed in the position papers during the open public consultation are provided below.

The company Apple supports the objective of ensuring a common approach and technical architecture for EU digital identity wallets, and urges the relevant European institutions to push for the adoption of international standards[4] as common standards for the EU digital identity framework and toolbox.

The Technical Committee on Electronic Signatures and Infrastructures (ETSI TC ESI) in France considers that this legislative proposal, the GDPR, the NIS2 Directive, and the digital markets and services acts mandate some providers with security and transparency requirements and the obligation to notify certain events that need coordination between the different supervision schemes, in order to avoid duplication that might generate doubt about which technical standards have to be followed.

The City of Stockholm emphasises that it is currently difficult for users to assess how their personal data will be used and which conditions apply, as well as to fully understand the regulations and conditions within this field. Moreover, it is not clear how the browser developers will be persuaded to comply with the new requirements and accept the new certificates. The City of Stockholm also highlights that the timeline for the proposal has to be realistic.

The company Microsoft refers to the need to coordinate existing and future EU legislation, such as the NIS2 and the Cybersecurity Act (e.g. regarding certification), to avoid regulatory overlap and inconsistencies.

Finance Denmark sees a risk of fragmentation of public/private solutions. To require private corporates to accept digital identity wallets for authentication purposes will require significant investment on behalf of financial institutions. Finance Denmark therefore proposes a solution based on ID switching: the eID would be the identification tool for online onboarding, while authentication for financial services would be based on a digital identity in a format that the individual bank supports.

The Certification Body of Deutsche Telekom Security GmbH states that differing requirements[5] leading to a distribution of responsibilities will probably result in different levels of service-security and service-assurance across the EU. They suggest putting an entity in place at EU level (such as the EU Agency for Network Information Security, ENISA) with binding effect, thereby ensuring harmonised interpretation and implementation of the amended eIDAS Regulation throughout Europe.

The European Digital SME Alliance recommends making it mandatory to publish references to standards, whenever possible, with implementing acts, and to introduce common rules for remote identification, so as to ensure a common approach to security and interoperability and to provide certainty for small and medium-sized companies to invest in eIDAS value-added services.

The company Eurosmart calls on the Commission to publish a new standardisation request on digital identity to support this proposal. Standards in digital identities are critical and should be developed in a fully transparent manner. According to Eurosmart, the European standardisation approach to digital identity has to prevent some actors from diverting the primary objectives of keeping personal data under citizens' control and watering down the 'security-by-design' principle.

Browser makers have expressed serious misgivings about supporting and displaying additional trust certificates. According to analysts, a lot of nuanced web infrastructure work would need to be done by third parties to interoperate with this EU requirement. Mozilla, for instance, is worried that the requirement would inadvertently expose EU residents to untenable security risks and roll back years of progress in security on the web.

The Germany identity security firm Onfido is worried about how the EU will handle the validation of an ID card issued by an EU Member State, the guarantee of the security of this ID card, and the linking of a person's physical identity with their digital ID card. Onfido also wonders how lost or compromised devices will be dealt with and whether the EU will allow third parties to access a digital identity with the user's permission. Onfido suggests increasing security by making it mandatory for governments to include a biometric authentication mechanism in their wallets.

The Foundation for Internet Domain Registration in the Netherlands (SIDN) welcomes the Commission's proposal, and highlights that any solutions should allow end-users to manage and control their digital identity, associated attributes and credentials in a free and open manner. SIDN is nevertheless worried that the proposal falls short in preventing identification means that are not free of charge to qualified and non-qualified trust service providers and does not prevent ID wallets from having secondary commercial purposes.

Legislative process

Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE); the rapporteur is Romana Jerković (S&D, Croatia). The committees for opinion are the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Legal Affairs (JURI) and the Committee on Civil Liberties Justice and Home Affairs (JURI).

The legislative process is in its early stages. On 17 June 2021, the European Commission presented the legislative proposal to Parliament's lead committee, ITRE. MEPs welcomed the proposal while raising some concerns on the digital divide and inclusion for those citizens who are less digitally literate, and the need to guarantee security and data protection in the systems chosen.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Negreiro M., The EU digital decade: A new set of digital targets for 2030, EPRS, European Parliament, August 2021.

Negreiro M., The NIS2 Directive: A high common level of cybersecurity in the EU, EPRS, European Parliament, February 2021.

Tuominen M. with Festor S., Establishing a framework for a European digital identity: Initial appraisal of a European Commission impact assessment, EPRS, European Parliament, October 2021.

OTHER SOURCES

European Digital Identity framework, European Parliament, Legislative Observatory (OEIL), European Parliament.

ENDNOTES

[1] In the context of the eIDAS Regulation, attributes refer to elements of personal information and data items from the individuals' identity criteria, such as nationality, sex, age, place of birth, etc.

[2] See Article 5c: 'Personal data shall be … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")'.

[3] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.

[4] Specifically, ISO 18013-5 (mobile driving licence or mDL) and 23220 (eID).

[5] For the interpretation of the eIDAS Regulation, with regard to legal and normative requirements, amended by the NIS2 Directive, GDPR/Regulation (EU) 2016/679 and Cybersecurity Act/Regulation (EU) 2019/881; and for the compliance assessment and/or certification of processes, systems and devices with segregation at EU and Member State levels.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

First edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.